

CLAIMS

1. A computer-implemented method for analyzing a virtual function, said method comprising:
  - 5       determining whether a virtual table exists for a virtual function;  
and  
      determining a call type for a virtual function.
2. The computer-implemented method for analyzing a virtual  
10   function as recited in Claim 1 further comprising the step of:  
      performing instrumentation on said virtual function based upon  
      said call type.
3. The computer-implemented method for analyzing a virtual  
15   function as recited in Claim 1 wherein said call type is selected from the  
      group comprising direct, indirect, and virtual.
4. The computer-implemented method for analyzing a virtual  
      function as recited in Claim 2 wherein the step of performing  
20   instrumentation on said virtual function based upon said call type  
      comprises:
  - provided said virtual table is located, replacing an existing address  
      for said virtual function with a new address for said virtual function in  
      said virtual table such that said new address points to instrumentation  
25   code;  
      upon a call to said virtual function, load said new address from said  
      virtual table such that execution is directed to the instrumentation code;  
      and  
      continue execution and execute said instrumentation code such  
30   that control is delivered to said instrumentor.
5. The computer-implemented method for analyzing a virtual  
      function as recited in Claim 4 further comprising:
  - performing a desired instrumentation task by said instrumentor;  
35   and  
      resume execution by said instrumentor at said existing address  
      previously contained in said virtual table.
6. The computer-implemented method for analyzing a virtual

function as recited in Claim 4 further comprising:

overwriting said instrumentation code with instrumentation code which performs a desired instrumentation task; and

provide an instruction at the end of said instrumentation code  
 5 wherein said instruction points back to said existing address previously contained in said virtual table.

7. The computer-implemented method for analyzing a virtual function as recited in Claim 1 further comprising:

10 determining from which location said virtual function has been called.

8. The computer-implemented method for analyzing a virtual function as recited in Claim 4 further comprising:

15 maintaining a mapping between said existing address for said virtual function and said new address for said virtual function.

9. A computer-readable medium embodying instructions that cause a computer to perform a method for analyzing a virtual function, said method comprising:

20 determining whether a virtual table exists for a virtual function; and  
 determining a call type for a virtual function.

25 10. The computer-readable medium of Claim 9 further comprising instructions that cause said computer to perform the step of:

performing instrumentation on said virtual function based upon said call type.

30 11. The computer-readable medium of Claim 9 wherein said call type is selected from the group comprising direct, indirect, and virtual.

12. The computer-readable medium of Claim 10 further comprising instructions that cause said computer to perform the steps of:

35 provided said virtual table is located, replacing an existing address for said virtual function with a new address for said virtual function in said virtual table such that said new address points to instrumentation code;

upon a call to said virtual function, load said new address from said

virtual table such that execution is directed to the instrumentation code;  
and

continue execution and execute said instrumentation code such  
that control is delivered to said instrumentor.

5

13. The computer-readable medium of Claim 12 further comprising  
instructions that cause said computer to perform the steps of:

performing a desired instrumentation task by said instrumentor;

and

10 resume execution by said instrumentor at said existing address  
previously contained in said virtual table.

14. The computer-readable medium of Claim 12 further comprising  
instructions that cause said computer to perform the steps of:

15 overwriting said instrumentation code with instrumentation code  
which performs a desired instrumentation task; and

provide an instruction at the end of said instrumentation code  
wherein said instruction points back to said existing address previously  
contained in said virtual table.

20

15. The computer-readable medium of Claim 9 further comprising  
instructions that cause said computer to perform the step of:

determining from which location said virtual function has been  
called.

25

16. The computer-readable medium of Claim 12 further comprising  
instructions that cause said computer to perform the step of:

maintaining a mapping between said existing address for said  
virtual function and said new address for said virtual function.

30

17. An apparatus for analyzing a virtual function, said apparatus  
comprising:

means for determining whether a virtual table exists for a virtual  
function; and

35 means for determining a call type for a virtual function.

18. The apparatus of Claim 17 for analyzing a virtual function, said  
apparatus further comprising:

means for performing instrumentation on said virtual function

based upon said call type.

19. The apparatus of Claim 17 for analyzing a virtual function wherein said call type is selected from the group comprising direct,  
5 indirect, and virtual.

20. The apparatus of Claim 18 for analyzing a virtual function, said apparatus further comprising:

means for replacing an existing address for said virtual function  
10 with a new address for said virtual function in said virtual table such that said new address points to instrumentation code, provided said virtual table is located;

means for loading said new address from said virtual table such that execution is directed to the instrumentation code, upon a call to said  
15 virtual function; and

means for continuing execution and executing said instrumentation code such that control is delivered to said instrumentor.

21. The apparatus of Claim 20 for analyzing a virtual function, said  
20 apparatus further comprising:

means for performing a desired instrumentation task by said instrumentor; and

means for resuming execution by said instrumentor at said existing address previously contained in said virtual table.

22. The apparatus of Claim 20 for analyzing a virtual function, said apparatus further comprising:

means for overwriting said instrumentation code with instrumentation code which performs a desired instrumentation task;  
30 and

means for providing an instruction at the end of said instrumentation code wherein said instruction points back to said existing address previously contained in said virtual table.

23. The apparatus of Claim 17 for analyzing a virtual function, said apparatus further comprising:

means for determining from which location said virtual function has been called.

24. The apparatus of Claim 20 for analyzing a virtual function, said apparatus further comprising:

means for maintaining a mapping between said existing address for said virtual function and said new address for said virtual function.